Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Sunday, September 16, 2007

Tamper evident numbers

From The Playdough Protocols:

> Evolving beyond clay tokens, accounting was the first use of the external marks and started to take a familiar form. Along with the tamper evident clay, the Sumerians developed a kind of virtual tamper evidence. It took the form of two sets of numbers. On the front of the tablet, each group of commodities would be recorded separately -- For example on the front would be recorded 120 pots of wheat, 90 pots of barley, and 55 goats. On the reverse would simply be recorded "265" -- the same objects counted gain, probably in a different order, and without bothering to categorize them. The scribe, or an auditor, would then verify that the sum was correct. If not, an error or fraud had occured. Note the similarity to tamper evident seals -- if a seal is broken, this meant that error or fraud had occured. The breaker of the seals, or the scribe who recorded the wrong numbers, or the debtor who paid the wrong amounts of commodities would be called on the carpet to answer for his or her discrepancy.
>
> Checksums still form the basis of modern accounting. Indeed, the principle of double entry bookeeping is based on two sets of independently derived numbers that must add up to the same number. Below, we will see that modern computers, using cryptographic methods, can now compute unspoofable checksums.

Posted by Nick Szabo at 2:12 PM

3 comments:

Citizen Dave said...

The story of the tallies also shows how low-technology tamper-evidence provides the basis for a payment system.

http://www.arraydev.com/commerce/jibc/9811-11.htm

9:53 AM

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

nick said...

That's an interesting article. One point of variance -- tallies were in use long before the Norman invasion, and probably date from very prehistoric times. For example, some notched bones from before 10,000 BC have been found that are probably tallies. Particuarly interesting for tallies, which may be of more recent invention than prehistoric times, is the splitting protocol (each side gets half of the tally stick split lengthwise).

11:03 AM

Daniel A. Nagy said...

The theory of cryptographic checksums (also known as hash functions or message digests) is still in its infancy. While they are arguably the most important tool in the financial cryptographer's toolbox (precisely for the reasons highlighted by this article), we know surprisingly little about them.
Most of the presently used constructs are showing weaknesses and even the criteria by which to evaluate new designs are not as clear as in the case of block ciphers.
NIST launched an international initiative to address the issue. Hopefully, this will generate more interest and more research in this very important (and very difficult) branch of cryptography.

6:18 PM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ▼ 2007 (47)
  - ► December (1)
  - ► October (2)
  - ▼ September (8)
    - Secure time broadcast
    - Real options analysis for space projects
    - Tamper evident numbers
    - Mining the vasty deep (iii)
    - Partial and total orders
    - Institutional changes prerequisite to the industri...
    - Secure property titles
    - Bilinear group cryptography
  - ► August (10)
  - ► July (4)
  - ► June (4)
  - ► May (8)
  - ► April (1)
  - ► March (2)
  - ► February (4)
  - ► January (3)
- ► 2006 (130)
- ► 2005 (44)

Simple theme. Powered by Blogger.